Información general

Pilz GmbH & Co. KG
Felix-Wankel-Straße 2
73760 Ostfildern
Deutschland/Germany
www.pilz.com

16 de mayo de 2024

Protección para empresas, máquinas y productos

Seguridad y Protección Industrial (Industrial Security): todo de un mismo proveedor

Ostfildern, 16 de mayo de 2024 - **Los incidentes de protección industrial han dejado de afectar solo a los sistemas informáticos para extenderse paulatinamente también al entorno de producción (OT). En el ámbito de la protección industrial (Industrial Security) se consideran incidentes tanto los ataques dirigidos como las manipulaciones inconscientes. El objetivo de la protección industrial en la producción es garantizar la disponibilidad de máquinas e instalaciones y la integridad y confidencialidad de los datos y procesos de las máquinas. En definitiva: Si una empresa no tiene el control sobre sus datos, está en juego la propia empresa y la seguridad de los trabajadores: sin protección no hay seguridad y, sin seguridad, las personas quedan desprotegidas.**

En la UE, la legislación ha reaccionado a las crecientes amenazas: A nivel de corporaciones, la **Directiva de seguridad de las redes y los sistemas de información NIS2** exige la implementación de un sistema integral de gestión de la seguridad de la información.

En el nuevo **Reglamento de Máquinas 2023/1230** ya se prevé la protección contra corrupción para máquinas e instalaciones y exige medidas de protección industrial para las partes de la máquina que influyen en la seguridad funcional.

El Reglamento **Cyber Resilience Act (CRA)** exige medidas de protección industrial para productos que contienen elementos

digitales. Esto incluye controles, sistemas E/S y diversos componentes que se montan en las máquinas.

Empresas, máquinas y productos: fabricantes y usuarios de máquinas deben afrontar retos y marcos jurídicos diferentes en cada uno de los niveles.

Independientemente del hecho de que el legislador obligue a implementar la protección industrial (Industrial Security), hay una serie de buenas razones para abordar el tema y dejarse asesorar con antelación. Porque muchos de los procesos y contextos de funcionamiento de máquinas propician manipulaciones y deben cuestionarse y modificarse urgentemente. La larga vida útil de muchas máquinas, por ejemplo, favorece en muchos casos la obsolescencia de los sistemas asociados y que llegue un momento en el que no correspondan a los estándares de protección actuales. Estos sistemas tienen brechas de seguridad que no se pueden cerrar porque el proveedor ha dejado de proporcionar actualizaciones de la protección. Muchas veces tampoco es posible implementar la protección contra software malicioso (malware) en los equipos terminales porque éstos han quedado obsoletos y podría afectar a su rendimiento, con el consiguiente riesgo de paradas de la producción.

Extensa oferta de servicios de Pilz

Se trata, en definitiva, de garantizar la protección de las operaciones comerciales, para lo cual las empresas deberán superar diferentes retos: desde la identificación de las normativas aplicables, la detección y solución de vulnerabilidades en los sistemas hasta la concienciación y formación de los empleados y posterior implantación de controles. Al ser la protección industrial (Industrial Security) un objetivo "móvil", se requiere además una verificación periódica del estado de protección industrial de la maquinaria.

La empresa de automatización Pilz ha hecho suyos estas exigencias y preparado para fabricantes y usuarios de máquinas de todo el mundo una oferta de servicios que considera todos los aspectos relativos a la protección de personas y máquinas desde una perspectiva holística. La oferta abarca desde información básica, guías de orientación y cursos de formación hasta el servicio Industrial Security Consulting Service (ISCS), en el que se ejecutan proyectos específicos.

Desde el año pasado, Pilz ofrece la cualificación "CESA – Certified Expert for Security in Automation", un curso de formación de dos días de duración que proporciona a los participantes conocimientos compactos sobre seguridad basados en las normas más recientes. A su vez, se abordarán medidas prácticas para la reducción de riesgos, como el control del acceso, el aumento de la seguridad de la red a través de medios técnicos, así como medidas organizativas para reducir los riesgos de seguridad. Tras superar el examen, los participantes obtienen el certificado TÜV-NORD mundialmente reconocido "CESA – Certified Expert for Security in Automation".

Con la nueva oferta de servicio Industrial Security Consulting Service (ISCS), Pilz amplía el análisis de seguridad de la maquinaria en el sentido de un visión holística de la seguridad y la protección. Basándose en la acreditada metodología de servicios en el ámbito de la seguridad funcional de las máquinas y en la serie de normativas de protección IEC 62443, Pilz ha desarrollado una gama de servicios que, una vez implantados, garantizarán que las empresas estén bien equipadas en materia de protección industrial (Industrial Security) y cumplan los requisitos legales vigentes.

Cuatro módulos para más protección industrial (Industrial Security)

El ISCS está compuesto por cuatro módulos: Análisis de necesidades de protección, evaluación de riesgos de protección industrial, concepto de protección industrial y verificación del sistema de protección industrial.

En el análisis de necesidades de protección, los expertos de Pilz determinan en la empresa cliente la demanda de protección de los diferentes "activos" (Assets) de la máquina o instalación. En la siguiente fase de evaluación de riesgos, se analizan los distintos riesgos y la probabilidad de que ocurran, teniendo en cuenta además todas las subsecciones y el ciclo de vida completo del sistema. A continuación, los expertos de Pilz estudian con el cliente enfoques de solución para contrarrestar los riesgos identificados y los posibles peligros.

En la tercer fase, los expertos de Pilz elaboran un concepto de protección industrial con estrategias y medidas para la defensa y mitigación de los riesgos derivados de ataques, manipulaciones y errores de mando. A esto se suma la definición de políticas, normas y directrices con el fin de asegurar la seguridad de funcionamiento y de diseño del sistema. En la última fase, la verificación del sistema de protección industrial, se comprueba la eficacia de las contramedidas implementadas.

Asegurar la disponibilidad de las máquinas

Industrial Security Consulting Service ayuda a mitigar e impedir ciberataques. Disminuye además el número de incidentes de protección de provocados de manera no intencionada. Esto, a su vez, aumenta la disponibilidad de la máquina y, en última instancia, reduce costes y asegura la rentabilidad.

Y, sobre todo, a través del ISCS se introducen medidas de protección adecuadas que garantizan la seguridad de las personas que trabajan en la máquina. Porque un incidente de protección puede convertirse en un obstáculo para las medidas de seguridad. Una barrera fotoeléctrica instalada, por ejemplo, delante de la maquinaria garantiza tiene la misión de evitar que el operario entre en una zona peligrosa. Si un intruso puede influir en el control y el mecanismo correspondiente, no podrá garantizarse la función de protección de la barrera fotoeléctrica. Aquí, la protección protege la seguridad.

Los fabricantes y usuarios de máquinas obtienen de Pilz un paquete de servicios que considera todos los aspectos relativos a la protección de personas y máquinas.

Por tanto, si hablamos de la implementación en la propia máquina, es ventajoso y conveniente considerar conjuntamente la seguridad y la protección. Y es que sin protección no hay seguridad y, sin seguridad, las personas quedan desprotegidas.

Regulado de forma transparente: ¿quién puede hacer qué en la máquina?

La seguridad de una máquina y de sus operadores depende de la regulación del acceso, ya sea de personas o de redes. Los puntos de acceso deberán estar protegidos contra la entrada no autorizada, por ejemplo, para que no puedan permanecer personas en la zona peligrosa mientras la máquina esté en funcionamiento. Si un operador autorizado se encuentra en esta zona de peligro para realizar tareas de mantenimiento, deberá garantizarse que ninguna otra persona pueda tener acceso al sistema durante este tiempo. Y es que incluso la operación o el mantenimiento bienintencionado de una instalación - ya sea in situ o a través de una red - pueden tener consecuencias fatales.

En este sentido es fundamental disponer de un Identification and Access Management (I.A.M.) como elemento que regule claramente los permisos y accesos a máquinas e instalaciones en la empresa. Esto incluye medidas organizativas y especificaciones, así como las funciones de seguridad pertinentes. Un sistema de autorización de acceso como PITreader de Pilz representa el componente de producto idóneo. Permite a los usuarios cumplir los requisitos de protección de trabajadores, responsabilidad civil, máxima productividad y protección de datos.

Con el sistema de autorización de acceso y selección de modos de operación PITmode fusion, Pilz brinda máxima flexibilidad para la selección funcional segura del modo de operación y la gestión de la autorización de acceso a máquinas e instalaciones. Cada operador tiene almacenados en un transpondedor con código RFID los permisos de acceso a máquinas acordes a sus aptitudes y cualificaciones. Por tanto, la instalación sólo puede ser utilizada y controlada por personal autorizado en modos de operación definidos. El resultado es un alto nivel de seguridad contra acciones no intencionadas y manipulaciones.

Si el sistema de autorización de acceso y selección de modos de operación se amplía con los componentes de un sistema modular de protección de puertas, se obtiene un concepto de acceso coherente a la máquina en términos tanto de seguridad como de protección.

El mejor sistema de protección de puertas no sirve de nada si los datos, conocimientos y procesos operativos no están adecuadamente protegidos contra accesos no autorizados y manipulación y permiten la entrada de intrusos en el sistema de control.

Industrial Firewall protege contra accesos desde el exterior

La función del Industrial Firewall SecurityBridge de Pilz es proteger el acceso desde fuera a las redes de automatización. Supervisa el flujo de datos entre el PC y el control y reduce así las posibilidades de ataque de piratas informáticos y de manipulación. SecurityBridge no solo protege contra posibles manipulaciones los controles de Pilz, sino también los de otros fabricantes.

En Pilz tenemos la convicción de que solo un enfoque holístico de seguridad y protección puede garantizar una protección integral de personas y máquinas. El hecho de que una empresa adopte medidas de seguridad ya no es una cuestión que queda a discreción de la empresa. Ahora es un requisito legal. En el sector de la construcción de máquinas, la protección industrial (Industrial Security) no es solo responsabilidad del Departamento de Informática, sino que debe ser un elemento integrado desde el diseño hasta la construcción. Implantar la seguridad a posteriori es laborioso y suele afectar a la facilidad de uso, la funcionalidad y la productividad.

((Caracteres: 10.173))

((cuadro:))

Resumen de la legislación de la UE en materia de protección industrial (Industrial Security):

Sobre todo en Europa, los legisladores están respondiendo a la situación de amenaza con una serie de leyes. Tanto es así que Europa tiene la normativa más estricta del mundo en este ámbito. Pero la coordinación con otros países ya está en marcha, y esas leyes también llegarán allí. Por tanto, cabe esperar una

uniformización de la protección industrial (Industrial Security) en todo el mundo.

NIS2: Más obligaciones para las empresas

La NIS (Seguridad de las redes y de la información) es una Directiva de la Unión Europea para reforzar la ciberseguridad. Esta directiva está en vigor desde 2016 y hasta ahora se aplicaba a los proveedores de servicios esenciales, como la energía, el transporte, la banca, las infraestructuras de los mercados financieros, el sector sanitario, el suministro y la distribución de agua potable y las infraestructuras digitales. Los proveedores de estos sectores debían tomar "medidas de seguridad adecuadas" y notificar los incidentes graves de seguridad. La nueva Directiva UE 2022/2555 (NIS2) de seguridad de las redes y los sistemas de información 2 obligará en el futuro a muchas más empresas a aplicar medidas de gestión de riesgos para la ciberseguridad. La NIS2 amplía los sectores e incluye, por ejemplo, la industria manufacturera/productora, incluidos los constructores de máquinas y los fabricantes de equipos eléctricos.

Se exigen análisis de riesgos y conceptos de seguridad para sistemas de información, así como la protección de la cadena de suministro y la seguridad del personal. Incluye también conceptos de control de acceso y la gestión de instalaciones, además de cursos de formación obligatorios para directivos.

La Directiva fue aprobada a finales de 2022 por el Parlamento Europeo y el Consejo de la UE. Como todas las Directivas UE, la NIS2 no es directamente efectiva y vinculante en los distintos Estados miembros de la UE, sino que debe ser transpuesta a derecho nacional en cada Estado. Los Estados miembros tienen de plazo hasta el 18.10.2024 para transponer la Directiva a derecho

nacional. Las empresas deberían preocuparse por cumplir la NIS2 lo antes posible y llevar a cabo una evaluación completa de la seguridad de la empresa. Esto incluye, por ejemplo, el establecimiento de un sistema de gestión de la seguridad de la información (SGSI). En este contexto, resulta útil la certificación conforme a la norma de seguridad de la información ISO 27001.

Ejemplo de aplicación de la NIS2 - aerogeneradores y parques eólicos: Los requisitos de la NIS2 afectan también al sector de la construcción de máquinas, como los fabricantes de instalaciones para la generación de energía (por ejemplo, aerogeneradores). Por su parte, el fabricante del aerogenerador necesitará soluciones de automatización, controles o sensores. Además, a partir de cierto tamaño, los fabricantes de componentes eléctricos también entran en el ámbito de aplicación de la NIS2. Puesto que la NIS2 establece que también hay que tener en cuenta a los proveedores, una empresa como Pilz deberá preocuparse por garantizar la seguridad de las cadenas de suministro y establecer normas para sus proveedores. Por tanto, la NIS2 abarca toda la cadena de suministro.

El nuevo Reglamento de Máquinas: Sin protección no hay marcado CE

La Directiva de Máquinas 2006/42/CE reviste especial importancia en el contexto de la seguridad funcional de las máquinas.

Para poder importar máquinas en Europa, los fabricantes de máquinas siempre han tenido que realizar un procedimiento de evaluación de la conformidad y obtener el Marcado CE al final del proceso.

En junio de 2023 se publicó el nuevo Reglamento de Máquinas, que recoge las especificaciones adaptadas al estado actual de la técnica. Al tratarse de un reglamento, no es necesario transponerlo antes a la legislación nacional. Los fabricantes de máquinas tienen de plazo hasta el 20.01.2027 para adaptarse a las nuevas exigencias y poder cumplirlas en la fecha de referencia.

Este Reglamento de Máquinas sustituye a la anterior Directiva relativa a las máquinas y se diferencia de ella en que introduce la obligatoriedad de la ciberseguridad. Mientras que la Directiva de Máquinas se limitaba a consideraciones sobre la seguridad, el Reglamento incluye el objetivo de protección industrial en el apartado "Protection against corruption" (Protección contra la corrupción) de los "Essential health and safety requirements (EHSR)" (Requisitos esenciales de salud y seguridad): Además, establece que las funciones de seguridad de la máquina no deben verse perjudicadas por falsificaciones involuntarias o intencionadas.

Esta nueva vía para obtener el Marcado CE plantea una serie de problemas e interrogantes para los fabricantes y empresas usuarias de máquinas, que tendrán que revisar sus actuales conceptos de seguridad y protección.

Cyber Resilience Act: protección industrial durante el ciclo de vida completo de la máquina

Además del análisis de la empresa y de las máquinas, es imprescindible implementar también medidas de protección directamente en los dispositivos (p. ej., controles). En septiembre de 2022, la Comisión Europea presentó un borrador de reglamento cuyo objetivo es aumentar la ciberseguridad de los productos. El "Cyber

Resilience Act" (CRA) está dirigido a fabricantes de productos que contienen elementos digitales (hardware y software) diseñados para comunicarse con otros productos. Esto afecta tanto a los productos del segmento B2C, como los teléfonos inteligentes (smartphones) y robots aspiradores, como a los del segmento B2B, como controles y sensores, así como a productos de software puro, como sistemas operativos, o la propia máquina.

El impacto real del CRA dependerá de los criterios que se utilicen finalmente para clasificar los productos. Según el CRA, solo podrán comercializarse productos que garanticen un nivel adecuado de ciberseguridad, y esto durante el ciclo de vida completo de un producto. La protección comienza, por tanto, en la fase de desarrollo del producto. Hace ya algunos años que Pilz basa sus procesos de desarrollo también en la normativa IEC 62443-4-1 "Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements", como demuestra el hecho de que SecurityBridge se ha desarrollado según criterios manifiestamente seguros.

((Caracteres: 5.826))

Ilustraciones

Fig. 1:

Grafik_aus_Prospekt_Schulungen_mit_Pilz_3c_ppt

Seguridad y Protección del mismo proveedor: Pilz dispone de una extensa oferta de soluciones con servicios y productos para la protección industrial (Industrial Security) en la máquina.

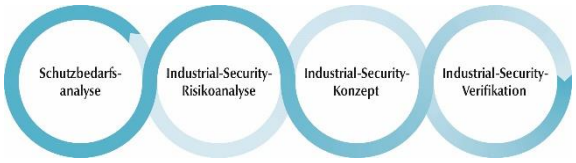
Fig. 2:

F_Services_ISCS_two_men_tablet_in_discussion_get1150297892_cold1_v0

Pilz lanza su oferta de servicio Industrial Security Consulting Service y ayuda a las empresas a proteger sus máquinas e instalaciones.

Fig. 3:

G_Cycle_Industrial_Security_de_v0



El paquete de servicios Industrial Security Consulting Service de Pilz se compone de cuatro módulos: Análisis de necesidades de protección, evaluación de riesgos de protección industrial, concepto de protección industrial y verificación del sistema de protección industrial.

Fig. 4:

F_Press_IAM_Man_using_PITreader_Key_Get1169337234_Get1169337153_cold1_v2

Un completo sistema Identification and Access Management gestiona el acceso a la aplicación y garantiza con ello la integridad de las funciones y medidas de seguridad; seguridad y protección industrial (Industrial Security) incluidas.

Fig. 5:

F_security_robot_man_virtual_world_Fot208731449_cold1_2019_06_v2

Protección industrial (Industrial Security) describe la protección de instalaciones de producción e industriales contra fallos de origen intencionado y no intencionado. El objetivo es garantizar la disponibilidad de máquinas e instalaciones y la integridad y confidencialidad de los datos y procesos de las máquinas.

Pilz – The Spirit of Safety

Pilz es proveedor mundial de productos, sistemas y servicios de técnicas de automatización. Como pionero en automatización segura, Pilz garantiza la seguridad de las personas, de las máquinas y del medio ambiente. Además de la sede central en Ostfildern (Stuttgart), esta empresa familiar fundada en 1948 cuenta hoy con 2.500 empleados en 42 filiales y sucursales distribuidas por todos los continentes.

El líder tecnológico ofrece una gama de soluciones de automatización completas para seguridad (Safety) y protección industrial (Industrial Security) a pie de máquina. El abanico incluye sensores, tecnología de control y accionamiento y sistemas para comunicación, diagnóstico y visualización industrial. Una oferta internacional de servicios que incluye asesoramiento, ingeniería y cursos de formación completa el programa. Las soluciones de Pilz se emplean no solo en la construcción de máquinas e instalaciones, sino también en muchos otros sectores, como la intralogística, el embalaje, la tecnología ferroviaria y la robótica.

www.pilz.com

Pilz en las redes sociales:

En nuestros canales de redes sociales ofrecemos información general sobre la empresa y las personas que trabajan en Pilz e informamos sobre temas de actualidad del mundo de las técnicas de automatización.

www.pilz.com/facebook
www.pilz.com/X
www.pilz.com/xing
www.pilz.com/youtube
www.pilz.com/linkedin

Contacto para la prensa:

Martin Kurth

Prensa corporativa y especializada
Tel.: +49 711 3409-158
m.kurth@pilz.de

Sabine Karrer

Prensa corporativa y especializada
Tel.: +49 711 3409-7009
s.skaletz-karrer@pilz.de

Eva Rössle

Prensa especializada

Tel.: +49 711 3409-7147
e.roessle@pilz.de

Hansjörg Sperling-Wohlgemuth
Dirección de congresos y conferencias
Tel.: +49 711 3409-239
h.sperling@pilz.de